REMARKS

Claims 1 to 29 are pending in the application, with Claims 1 to 6, 8 and 10 to 15 having been amended, and with Claims 16 to 29 having been added. Claims 1, 11, 12 and 22 are the independent claims. Reconsideration and further examination are respectfully requested.

Claims 1, 3, 5 to 7 and 13 to 15 were rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 6,543,052 (Ogasawara) in view of U.S. Patent No. 5,530,758 (Marino, Jr.); and Claims 2, 4 and 8 to 12 were rejected under § 103(a) over Ogasawara in view of Marino, Jr., and further in view of U.S. Patent No. 6,385,655 (Smith). Reconsideration and withdrawal of these rejections are respectfully requested.

Turning to specific claim language, amended independent Claim 1 is directed to a method for the secure printing of print data from a client application residing on a data network to an interface device which has a printer, the interface device residing on a digital cable network which has a cable head end for interfacing the digital cable network to the data network. The method includes the steps of generating print data in the client application, determining whether a secure communication path exists between the client application and the interface device, transmitting, in response to a determination that the secure communication path exists, the print data from the client application to the interface device, and sending the print data from the interface device to the printer for printing.

The cited art, namely Ogasawara and Marino, Jr., is not seen to disclose or suggest the foregoing features of amended independent Claim 1, particularly with respect to at least the features of generating print data in the client application, determining whether a secure communication path exists between the client application and the interface device, and

transmitting, in response to a determination that the secure communication path exists, the print data from the client application to the interface device.

It is alleged in the Office Action that Ogasawara teaches the aforementioned mentioned features, except for the feature of determining whether a secure communication path exists between the client application and the interface device. Applicants strongly disagree with this assertion. Ogasawara is seen to teach a method for providing internet access and internet shopping features in a digital cable environment, in which the user can purchase items over the internet using features such as voice and bar code recognition built into the remote control unit and the interface device. (Ogasawara, abstract; Figs. 3, 5A & 5B; and column 2, lines 13 to 44). With the invention described in Ogasawara, the user can purchase items over the internet using voice commands or by scanning a bar code of an item (Ogasawara, abstract; column 1; lines 61 to 65; column 3, lines 14 to 23; and column 5, lines 54 to 65). However, Ogasawara is not seen to disclose or suggest generating print data in a client application residing on a data network.

The client application of the present application is distinct from the specific purpose-type application software that includes voice recognition software and bar code recognition software as described in Ogasawara (Ogasawara, column 3, lines 14 to 23). In this regard, there is no mention of generating print data anywhere in the method described by Ogasawara. In the art described by Ogasawara, the purpose of the specific purpose-type application software is to allow an alternative means for the user to communicate to the interface device to purchase merchandise over the internet, as opposed to only using a keyboard as an input method. The method of Ogasawara is not seen to disclose or suggest generating print data in a client application, where the client application resides on a data network separate from the cable head end.

It is also alleged in the Office Action that the method of Ogasawara discloses generating and sending print data to a printer connected to an interface device. Applicants strongly disagree with this assertion. Ogasawara is seen to disclose an interface device that has an external interface that can be connected to peripherals such as a printer, but there is not seen to be any mention in Ogasawara of where the print data is generated for printing on the printer. (Ogasawara, Fig. 1; and column 2, lines 41 to 44). The disclosure of having an external interface for connection to a printer is not seen in anyway to disclose or suggest the generation of print data in a client application which resides on a data network separate from the cable head end.

As stated in the Office Action, Ogasawara is not seen to disclose or suggest determining whether a secure communication path exists between the client application and the interface device. Accordingly, it is not seen to be possible for Ogasawara to disclose or suggest transmitting, in response to a determination that the secure communication path exists, the print data from the client application to the interface device and then sending the print data from the interface device to the printer for printing. Ogasawara is seen to disclose a method for the sending of voice data from the interface device to the remote control unit, wherein the voice data is converted to analog voice data which is transmitted through a speaker on the remote control unit to the user. (Ogasawara, column 5, lines 53 to 65). transmission of voice data is not seen in any way to disclose or suggest transmitting, in response to a determination that the secure communication path exists, the print data from the client application to the interface device. There is not seen to be any mention in Ogasawara of checking for the presence of a secure communication path, much less determining whether to send print data from a client application to the interface device based on whether or not such a secure communication path exists. Furthermore, the disclosure in Ogasawara of an interface device which is only seen to control a

peripheral such as a printer and has an external interface with a peripheral is not seen to in any way disclose or suggest transmitting print data from the client application to the interface device, and sending the print data from the interface device to the printer for printing.

Marino, Jr. is not seen to remedy the foregoing deficiencies of Ogasawara, particularly with respect to the features of determining whether a secure communication path exists between the client application and the interface device. Marino, Jr. is seen to disclose a method of for secure communication between secure nodes in a computer network having unsecured nodes. (Marino, Jr., abstract; Figs. 1 & 2; and column 2, lines 7 to 24). In Marino, Jr., task 56 is seen to determine whether the destination entity is authorized to receive private data. (Marino, Jr., column 5, lines 42 to 44). According to Figure 5 in Marino, Jr., if the destination entity is authorized to receive private data, query task 60 determines whether secure link 30 is available for exchanging data with the destination entity. (Marino, Jr., Fig. 5). In determining whether secure link 30 is available, task 60 consults the lBAC table 48 in making its determination. (Marino, Jr., Fig. 4; and column 6, lines 62-66). However, the purpose of this determining step is either to secure an unsecured channel by passing the path name of the destination entity, and requesting a COMSEC secure channel initialization through security kernel 36 or to store information regarding the secure channel in channel ID table 68 by creating a channel ID and creating an association between the COMPUSEC attribute and the secure channel (Marino, Jr., column 6, lines 2 to 24 and lines 55 to 58).

With respect to amended independent Claim 1, the method disclosed by Marino, Jr. is not seen to disclose or suggest determining whether a secure communication path exists between the client application and the interface device for the purpose of transmitting, in response to a determination that the secure communication path exists, the print data from the

client application to the interface device, and sending the print data from the set top box to the printer for printing. The method according to Marino, Jr. and the method according to independent Claim 1 both contain a step of determining whether a secure communication path exists. However, the determining step of Marino, Jr. is not seen in any way to determine whether a secure communication path exists between a client application and an interface device for use in transmitting print data from the client application to the interface device for printing.

Based on the foregoing, Applicants respectfully submit that Ogasawara and Marino, Jr., either alone or in combination, for which combination no motivation or suggestion is seen to be present, are not seen to render obvious the invention of amended independent Claim 1 because those references are not seen to teach the combination of features of amended independent Claim 1. Amended independent Claim 1 is therefore believed to be in condition for allowance, and such action is respectfully requested.

In the Office Action, a combination of Shaffer and Smith is referenced with respect to the rejection of independent Claim 11. However, there were no references to any particular portion of Shaffer in the Office Action. Applicants presume that the Examiner was referring to the combination of Smith and Ogasawara concerning the rejection of independent Claim 11. If this is not the case, Applicants respectfully request clarification of the referenced art concerning the rejection of independent Claim 11.

With respect to specific claim language, amended independent Claim 11 is directed to a method for the secure printing of print data from a client application residing on a data network to an interface device which has a printer, the interface device residing on a digital cable network which has a cable head end for interfacing the digital cable network to the data network. The method includes the steps of generating print data in the client application,

determining that a secure communication path exists between the client application and the cable head end upon receipt through a secure protocol of a confirmation from the cable head end that the cable head end is a secure location, sending, in response to a determination that the secure communication path exists, the print data from the client application to the cable head end in a device-independent format, transforming in the cable head end, the print data from the device-independent format to a rasterized format which corresponds to the printer, determining that a secure communication path exists between the cable head and the interface device upon receipt, through a secure protocol, of a confirmation from the interface device that the interface device is a secure location, and sending, in response to a determination that the secure communication path exists, the print data in the rasterized format from the cable head end to the interface device for printing on the printer.

In this regard, amended independent Claim 11 is seen to include at least the features of amended independent Claim 1, in addition to other features. The applied art, Ogasawara, Marino and Smith, is not seen to teach or disclose the foregoing features of amended independent Claim 11, particularly with respect to determining that a secure communication path exists between the client application and the cable head end upon receipt through a secure protocol of a confirmation from the cable head end that the cable head end is a secure location, sending, in response to a determination that the secure communication path exists, the print data from the client application to the cable head end in a device-independent format, and determining that a secure communication path exists between the cable head and the interface device upon receipt, through a secure protocol, of a confirmation from the interface device that the interface device is a secure location, and sending, in response to a determination that the secure

communication path exists, the print data in the rasterized format from the cable head end to the interface device for printing on the printer.

Smith is seen to teach a method for securely delivering documents over an electronic network that uses special client applications on both the sender and recipient computers. (Smith, abstract; Figure 1; column 2, lines 58 to 67; and column 3, lines 1 to 15). In Smith, the sender is seen to use the special client application to send a file to server 22, and then the recipient, using the same special application, receives a notice, upon which the recipient computer can download the file from server 22. (Smith, column 5, lines 22 to 66). However, nowhere is Smith seen to disclose or suggest that server 22 transmits the print data to the recipient computer based upon the outcome of a determination of the secure status of the communication path to the recipient computer. The invention of Smith is simply seen to provide security for restricting access to the system by using security measures such as certificate authentication.

Smith is not seen to disclose or suggest determining that a secure communication path exists between the client application, the cable head end and the interface device upon receipt through a secure protocol of a confirmation from the cable head end that the cable head end and the interface device are secure locations, and sending, in response to a determination that the secure communication path exists, the print data from the client application to the cable head end to the interface device in a device-independent format.

Smith defines the term "document" as any contiguous collection of data including platform-independent formatted document such as an HTML, PDF, or Envoy document. (Smith, column 4, lines 65 to 67; and column 5, lines 1 to 11). However, Smith is not seen to disclose or suggest sending, in response to a determination that the secure communication path exists, the

print data from the client application to the cable head end to the interface device in a device-independent format and transforming in the cable head end, the print data from the device-independent format to a rasterized format which corresponds to the printer. Amended independent Claim 11 teaches the secure sending of rasterized print data as opposed to the sending of documents.

As discussed above with respect to amended independent Claim 1, Ogasawara is not seen to disclose or suggest generating print data in the client application, determining that a secure communication path exists between the client application, the cable head end, and the interface device, transforming in the cable head end, the print data from a device-independent format to a rasterized format which corresponds to the printer, and sending, in response to a determination that a secure communication path exists, the print data in a rasterized format from the client application, to the cable head end, to the interface device, for printing by the printer connected to the interface device.

In addition, also as discussed above, Marino, Jr. is not seen to remedy the deficiencies of Ogasawara, because Marino, Jr. is not seen to disclose or suggest determining whether a secure communication path exists between a client application and an interface device for use in transmitting print data from the client application to the interface device for printing.

Based on the arguments previously set forth, Applicants respectfully submit that Ogasawara, Marino, Jr. and Smith, either alone or in combination, are not seen to anticipate or render obvious the invention of amended independent Claim 11 because those references are not seen to teach the combinations of features of amended independent Claim 11. Amended independent Claim 11 is therefore believed to be in condition for allowance, and such action is respectfully requested.

Amended independent Claim 12 is directed to a method for the secure printing of print data from a client application residing on a data network to an interface device which has a printer, the interface device residing on a digital cable network which has a cable head end for interfacing the digital cable network to the data network, where the method includes the steps of generating print data in the client application, transforming, in the client application, the print data from the device-independent format to a rasterized format which corresponds to the printer, encrypting, in the client application, the print data in the rasterized format, sending the encrypted print data in the rasterized format from the client application to the cable head end, sending the encrypted print data in the rasterized format from the cable head end to the interface device, and decrypting, in the interface device, the print data in the rasterized format for printing on the printer.

The applied art, Ogasawara, Marino and Smith, is not seen to teach or disclose the foregoing features of amended independent Claim 12, particularly with respect to the features of transforming, in the client application, the print data from the device-independent format to a rasterized format which corresponds to the printer, encrypting, in the client application, the print data in the rasterized format, sending the encrypted print data in the rasterized format from the client application to the cable head end, sending the encrypted print data in the rasterized format from the cable head end to the interface device, and decrypting, in the interface device, the print data in the rasterized format for printing on the printer.

As discussed above, Ogasawara is not seen to be concerned with determining or ensuring a secure communication transfer from a client application to an interface device, much less performing encryption and decryption of print data for such a transfer. In this regard, Marino, Jr. is seen to teach a method of an integrity process 76 which verifies the integrity of the

software running on secure processor subsystem 34. (Marino, Jr., Figures 2 and 8). In Marino, Jr., when the application is loaded onto the subsystem, a checksum may be generated and compared against a given value to insure the integrity of the application, wherein the checksum is generated, encrypted, and decrypted by task 82. (Marino, Jr., column 7, lines 15 to 22). This method taught by Marina Jr. is not seen to disclose or suggest generating print data in the client application, transforming, in the client application, the print data from the device-independent format to a rasterized format which corresponds to the printer, encrypting, in the client application, the print data in the rasterized format, sending the encrypted print data in the rasterized format from the client application to the cable head end, sending the encrypted print data in the rasterized format from the cable head end to the interface device and decrypting, in the interface device, the print data in the rasterized format for printing on the printer.

In this regard, Marino, Jr. is not seen any where to generate, encrypt and decrypt rasterized print data. Rather, Marino, Jr. discloses a method of generating, encrypting, and decrypting a checksum of the application that is loaded on the subsystem. Also, Marino, Jr. is not seen to disclose or suggest a source to end encryption of rasterized print data. The rasterized print data according to amended independent Claim 12 is encrypted in the client application. The encrypted rasterized print data remains encrypted in the cable head end and it is then decrypted in the interface device for printing by the printer attached to the interface device. Again, this differs from the method of Marino, Jr. which is only seen to encrypt and decrypt the checksum of the application on the subsystem.

Smith is only seen to disclose the possibility of using various security methods, such as certificate authentication, for restricting access to the system to only authorized users. (Smith, column 20, lines 41 to 49). Nowhere is Smith seen to disclose or suggest the

combination of rasterization, encryption and decryption between a client application, cable head end and a set-top box as in amended independent Claim 12.

Based on the arguments set forth above, Applicants respectfully submit that Marino, Jr., Smith and Ogasawara, either alone or in combination, for which combination no motivation or suggestion is seen to be provided, are not seen to anticipate or render obvious the invention of amended independent Claim 12 because those references are not seen to teach the combinations of features of amended independent Claim 12. Amended independent Claim 12 is therefore believed to be in condition for allowance, and such action is respectfully requested.

Amended claims 13, 14 and 15 are directed to apparatus, computer-executable steps, process steps, and computer-readable medium claims, each of which substantially implements the method steps of Claims 1 to 12. Amended claims 13, 14 and 15 are therefore also believed to be in condition for allowance.

Newly-added independent Claim 22 is directed to a method for the secure printing of print data on a network comprising the steps of rendering print data, determining whether a secure communication path to an interface device which has a printer exists, transmitting, in response to a determination that the secure communication path exists, the rendered print data to the interface device via a network, and sending the rendered print data from the interface device to the printer for printing.

Based on the arguments set forth above, Applicants submit that the applied art, Ogasawara, Marino, Jr. and Smith, is not seen to disclose or suggest at least the step of determining whether a secure communication path to an interface device which has a printer exists and the step of transmitting, in response to a determination that the secure communication path exists, the rendered print data to the interface device via a network.

Therefore, Applicants respectfully submit that Marino, Jr., Smith and Ogasawara, either alone or in combination, are not seen to anticipate or render obvious the invention of newly-added independent Claim 22. Independent Claim 22 is therefore also believed to be in condition for allowance, and such action is respectfully requested.

The other pending claims in this application are each dependent from the independent claims discussed above and are therefore believed patentable for the same reasons. Because each dependent claim is also deemed to define an additional aspect of the invention, however, the individual consideration of each on its own merits is respectfully requested.

Based on the foregoing amendments and remarks, the entire application is believed to be in condition for allowance and such action is respectfully requested .

Applicants' undersigned attorney may be reached in our Costa Mesa, CA office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicants

Registration No. 40,595

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

CA_MAIN 71544 v 1